U.S. Department of Homeland Security

Office of State and Local Government Coordination and Preparedness

Tactical Interoperable Communications Planning Guidance and Template

Homeland Security

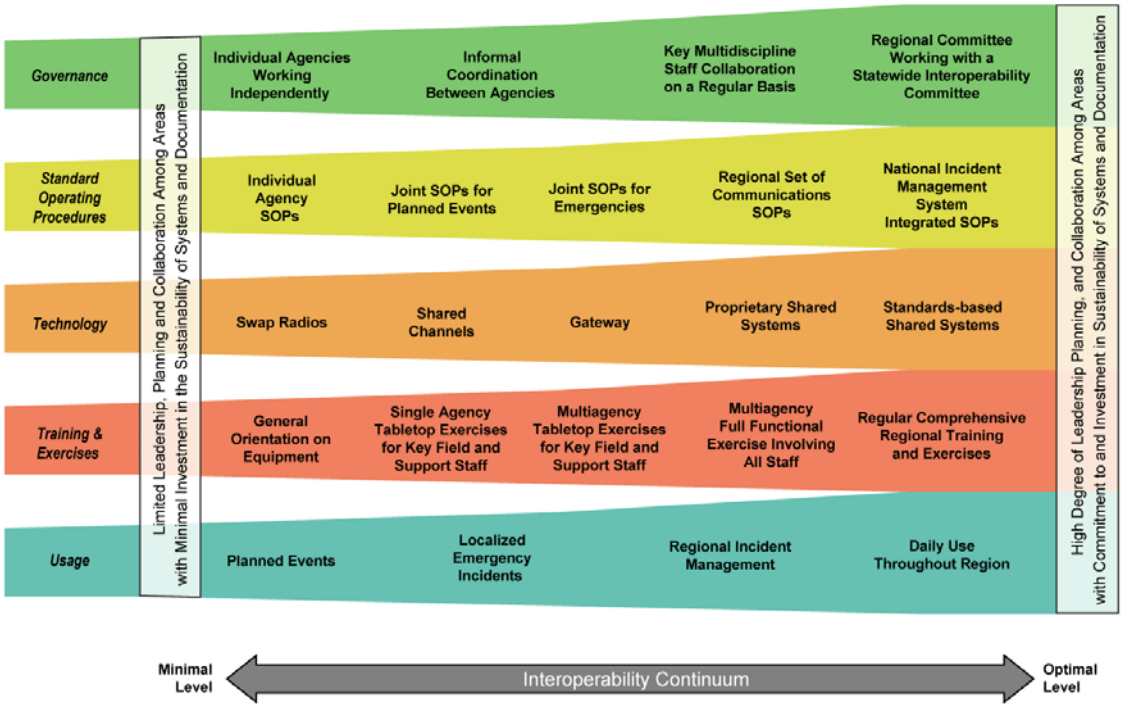
March 2005

Preface

This Tactical Interoperable Communications Plan guidance and template has been drafted for use by participants in the FY2005 Homeland Security Grant Program (HSGP). It has been created by the Department of Homeland Security (DHS) Office for Domestic Preparedness (ODP) in coordination with the SAFECOM program of the DHS Science and Technology Directorate's Office for Interoperability and Compatibility (OIC).

In May 2004, DHS launched the RapidCom initiative to help improve capabilities for immediate, tactical-level interoperable communications in ten high-threat urban areas. The OIC SAFECOM program and DHS ODP worked in cooperation with federal partners such as the Department of Justice's 25 Cities Project and the CommTech Program to provide assistance to incident commanders in each of these areas in order to improve their abilities to adequately communicate with each other and their respective command center within one hour of a major incident.

The work done in these urban areas through RapidCom revealed interoperability issues consistent with those found by the National Task Force on Interoperability (NTFI) such as incompatibility of equipment, the need for a governance structure, and a lack of planning and coordination. In response to these findings, SAFECOM developed a framework called the Interoperability Continuum to graphically depict the five critical elements of success—governance, standard operating procedures, technology, training & exercises, and usage of equipment—that must be addressed to develop robust interoperability solutions. This continuum framework encourages a shift from a technology-centric focus to a comprehensive operational focus on the key interoperability success factors.



The Continuum provided the foundation for the assistance that was provided to the ten urban areas for this initiative. As a result of this initiative, ODP elevated the value of tactical-level interoperability and inserted a new requirement into their grant packages: a requirement for grantees to develop plans that enable their communities to achieve, at a minimum, tactical-level interoperability. The basis for the plans the grantees will develop for tactical-level interoperability will also use the Continuum as a framework for planning. It is important to note that the Continuum is a tool that was developed for comprehensive interoperable communications planning and therefore all elements may not apply to urban area tactical interoperable communications plans. The guidance contained within this document reflects many of the Continuum's elements.

While the development of plans for incident management interoperability at a tactical level can provide an interim resolution to an area's interoperability needs, such solutions should always be in support of long term interoperability by building upon or accelerating long term strategies and efforts.

I. Tactical Interoperable Communications Plan

The FY05 HSGP provides funding for planning, equipment, training, exercises, and program management and administration to enhance preparedness to prevent, respond to, and recover from acts of terrorism. In an effort to facilitate the coordination and management of preparedness funding and enhance linkages to State and Urban Area Homeland Security Strategies, the FY05 HSGP integrates the following six programs into a single application kit and program guidance document: State Homeland Security Program, Urban Areas Security Initiative (UASI), Law Enforcement Terrorism Prevention Program, Citizen Corps Program, Emergency Management Performance Grants, and the Metropolitan Medical Response System.

Requirements

This document will provide an outline and basic guidance for HSGP grant recipients to create a Tactical Interoperable Communications Plan as required by the Fiscal Year 2005 HSGP Program Guidelines and Application Kit.

As part of this effort, each urban area receiving FY05 UASI funds must develop a plan to achieve tactical interoperable communications across jurisdictions in the urban area and test the plan through the cycle of exercise activity required for the Improvised Explosive Device (IED) scenario (see page 50 of the National Guidance). Each state that does not have a designated urban area must use the same multi-jurisdictional metropolitan area or region designated to test the prevention and response plans to meet the tactical interoperable communications requirements of the FY05 HSGP program.

Those UASI jurisdictions that developed plans in 2004 as part of their participation in the RapidCom initiative will submit the plan and validate that plan through the exercise requirement.

Assistance in developing this required Tactical Interoperable Communications Plan is available through ODP's Interoperable Communications Technical Assistance Program (ICTAP) on a first-come, first-serve basis. Inquiries about this support should be directed to your ODP Preparedness Officer or to the Centralized Scheduling and Information Desk (CSID) at 1-800-368-6498 or askcsid@dhs.gov.

Timetable

1. Tactical Interoperable Communications Plans must be submitted by all grantees no later than September 30, 2005.

2. Upon submission of the Plan, grantees will have ***one year*** to validate the plan as part of the cycle of multi-jurisdictional exercise activities required for the IED scenario.

II. Tactical Interoperable Communications Plan Guidance

Tactical interoperable communications is defined as the rapid provision of on-scene, incident based mission critical voice communications among all first-responder agencies (EMS, fire and law enforcement), as appropriate for the incident, and in support of an incident command system as defined in the National Incident Management System (NIMS) model. The chart at right shows many aspects of tactical interoperable communications that should be incorporated into the development of a Tactical Interoperable Communications Plan.

- Tactical interoperable communications may be provided through the use of common equipment (common channels, cached radios or shared systems) or a gateway between dissimilar systems and/or radio frequency bands;
- Tactical interoperable communications may use fixed and/or mobile/portable solution(s).
- Tactical interoperable communications must be rapidly deployable at any time (24/7)
- Tactical interoperable communications should be fully operational within an hour of an incident occurring.
- Tactical interoperable communications requires oversight by trained Communications Unit Leaders, as defined within the NIMS, to support equipment deployment.
- Tactical interoperable communications plans should always be in support of long-term interoperability by building upon or accelerating long-term strategies and efforts.

The Tactical Interoperable Communications Plan template is divided into six sections, most of which coincide with the elements of the Interoperability Continuum. The coinciding elements are noted in parentheses for your reference:

1. Urban Area Information
2. Governance Structure (Governance)
3. Interoperability Equipment (Technology)
4. Policies and Procedures for Interoperable Equipment (Standard Operating Procedures)
5. Incident Plan for Tactical Communications
6. NIMS Communications Unit Leader Training (Training and Exercises)

Information on each of these sections, as well as recommended steps to take in developing each component of the plan are detailed in the following sections.

Section 1 – Urban Area Information

The template requires a basic description of your Urban Area or metropolitan area designated by the State. Information to be provided about the site includes the following:

1. **Overview:** Provide a brief overview of the Urban Area/metropolitan area and its efforts in addressing interoperable communications. Consider all communications interoperability goals and objectives included in the UASI strategic plan to ensure tactical interoperable communication plans align with the overall strategy. Any challenges faced to date with communications should also be covered in this section.

2. **Included Agencies:** List all agencies represented in the Tactical Interoperable Communications Plan, including those agencies represented in the Urban Area Working Group (UAWG).

> **NOTE:** In some cases, sites have indicated that their communications interoperability efforts extend beyond the jurisdictions included in the Urban Area/metropolitan area. While not required, grantees are welcome to consider these additional agencies in the Tactical Interoperable Communications Plan.

3. **Tactical Interoperable Communications Plan Point of Contact:** Provide name and contact details for the primary point of contact (POC) who will be available to answer questions about this plan.

Section 2 - Defining Your Governance Structure

Governance refers to establishing a shared vision and an effective organizational structure to support any project or initiative that seeks to solve interoperability issues by providing guidance and support through common policies, processes, and procedures. Establishing a common governance structure will improve communication, coordination, and cooperation across the regions and disciplines that are essential in achieving an acceptable level of communications interoperability.

A formal governance structure will improve interoperability policies, processes and procedures by enhancing communications, coordination and cooperation, establishing guidelines and principles, and reducing any internal jurisdictional conflicts. It will identify and quantify fiscal and other resource requirements associated with the implementation of a tactical interoperability effort. This group should consist of representatives from local, tribal, state and federal entities, as well as from all pertinent public safety disciplines within the identified region.

For the purpose of this Tactical Interoperable Communications Plan, include the representatives who may be involved in the IED scenario. A formal governance structure is critical to the success of a Tactical Interoperable Communications Plan. A major advantage will be the level of jurisdictional and agency equality that it will bring to

the effort. If an existing interoperability committee is already in place, tactical planning may be the responsibility of a subgroup. In other cases, a tactical planning group will need to be newly created.

The Governance group, typically built upon a written agreement among all participating agencies and organizations, becomes the Regional Authority with overall responsibility for ensuring a successful tactical interoperability implementation within the region.

The following best practices are provided for you to consider in developing and/or enhancing your governance structure:

Membership: Members of the Governance group should:

- Be representative of all first responders, plus emergency management and Public Information (PIO - media relations is important in a terrorism incident).
- Include appropriate state and Federal agency representation (state police, FBI, Secret Service, etc).
- Include key leaders (agency heads with authority - budget and management - to implement the final plan).
- Be representative of all jurisdictions that would be considered for response.

Responsibilities: The Governance group may oversee a number of significant responsibilities, including:

- Establishing and managing other Committees, and staffing the overall process as necessary.
- Adopting final solution(s) and directing implementation.
- Providing commitment to sustaining the process once implemented (maintenance of equipment and SOPs, assuring training and exercises).

Meeting Schedule: Regular meetings of the Governance group are important during the initial planning process for regional interoperability in order to meet the responsibilities described above. Once tactical interoperable communications are in place, less frequent meetings are needed.

Agency Responsibilities and Rights: Specific responsibilities and rights of participating agencies must be clearly defined. This is typically done through a written agreement (e.g., Joint Powers Agreement, Memorandum of Agreement/Understanding, etc). The written agreement should address, among other issues:

- Providing Interoperability Assets
- Using Interoperability Assets
- Managing Interoperability Assets

- Problem Identification and Resolution

Regional Authority for Coordination and Assignment of Interoperability Assets: It is desirable to establish a 24/7 team that is given the authority to assign, coordinate and respond with regional interoperability assets. This team should include operational support, including personnel trained as Communications Unit Leaders, as defined in the NIMS model. The team should also include technical staff who are familiar with the detailed operation of interoperable equipment. A written agreement should be developed that describes:

- Authorized parties
- Responsibilities

Within your governance structure documented in the Plan, it is recommended that working groups focus on two key aspects of tactical interoperability:

Operational Working Group: Responsible for determining operational requirements, developing Standard Operating Procedures (SOPs) and coordinating training. Specific work group responsibilities could include:

- Review existing SOPs and apply as appropriate to anticipated incident(s).
- Develop formal written guidelines and checklists (SOPs) for an IED event. This can be expanded to include each element of Chemical, Biological, Radiological, Nuclear and Explosive (CBRNE) and all-hazard events later.
- Ensure that SOPs and checklists follow ICS/NIMS standards.
- Coordinate agency participating in NIMS Communication Unit Leader training.
- Coordinate with Technical Working Group as appropriate to include technical guidelines and checklists into written plans.

Technical Working Group: Responsible for identifying, developing and overseeing technical solutions. Specific work group responsibilities could include:

- Identify existing technical solutions, including appropriate and available equipment.
- Evaluate alternative solutions (either available or that can be purchased) with regard to potential incident types.
- Review potential solutions with Operational Working Group to identify most appropriate one(s) for anticipated types of incidents.
- Evaluate solution(s) through exercises (tabletop up to full-scale) to ensure selected solution(s) are workable in the field.

- In conjunction with Operational Working Group, prepare solution recommendation(s) and budget(s) for adoption by Governance Committee.

Section 3 - Interoperable Equipment

Technology refers to the equipment/infrastructure, network, and applications that public safety disciplines use to exchange critical information when responding to incidents. Although technology is a critical tool for improving interoperability, it is not the sole component of an optimal solution. Success in each of the other elements of the Continuum is essential for technology solutions to be implemented effectively. An optimal technology solution should be coupled with an operational environment in which responders use equipment on a regular basis, a formalized governance structure is established, responders are trained on communications-specific procedures, and interoperability plans and standard operating procedures are documented and used regularly for incident response.

Incompatible and aging communications equipment offers an obstacle to total interoperability. This is a common challenge that was originally outlined in the National Task Force on Interoperability's (NTFI) *Why Can't We Talk* document, released in February 2003. Different jurisdictions use different equipment and different radio frequencies that cannot communicate with one another. The radio and communications systems used by various agencies and jurisdictions are often at different stages of their life cycle. While agencies are familiar with their own communications equipment, and select personnel may have a basic understanding of the systems in place in the region, this information has rarely been documented for the overall UASI site or state region. This baseline inventory and documentation of interoperable communications equipment is fundamental to a successful tactical plan. Regional representatives should identify what resources exist within the region to support a multi-agency, public safety response to an incident.

The template divides interoperable equipment into the types identified by the SAFECOM program: swap radios, shared channels, gateways, and shared systems. Grantees should list all interoperable communications resources according to these categories, and indicate what agency is primarily responsible for the operation and maintenance of the equipment.

The template categories are:

1) Swap Radios

2) Shared Channels

3) Gateways

4) Shared Systems

Section 4 - Policies & Procedures for Interoperable Equipment

In many of the current UASI sites, agencies have procured equipment that is capable of providing interoperable communications. However, policies are rarely in place that document how communications would be provided in an IED incident. Policies and procedures addressing both operational and technical components are essential in the development and deployment of any solution. They enable first responders to act in a coordinated fashion across disciplines in the event of an emergency. In this section, grantees should document the policies and procedures that have been developed for their interoperable equipment.

Grantees should only complete policies and procedures for the types of interoperable equipment that they have included in Section 3 – Interoperable Equipment.

The following detailed guidance, based on best practices from state and local agencies, has been compiled to assist grantees in developing policies and procedures for each type of interoperable equipment.

1) Swap Radios:

One way to provide interoperability among agencies jointly responding to an incident is to have on-scene responders from all agencies swap their incompatible radios with those from a radio cache. This allows all responders to use a common, compatible set of radios. For a radio cache to be an effective shared resource, it should have the following characteristics:

- Be fully charged and maintained, ready for deployment at all times.
- Include extra charged batteries for extended deployments.
- Personnel available to transport the radios to the incident scene.
- Technicians available for on-scene support during the deployment.
- Check-out and tracking procedures during the incident to ensure the radios are properly returned to the cache following the incident.

Rules of Use: The following are some rules of use that may be included in this section. These examples are not exhaustive. The region should include any rules of use in this section that will apply to radio caches, including:

- National Incident Management System compliance.
- Use of plain language (no radio codes).
- Use of Unit Identification.
- Use of encryption / no encryption.

NOTE: Based on best practices / lessons learned from emergency responders, encryption should be used only if the agencies involved have established that it will not prevent successful interoperability.

Interoperable Communications Request: This section should detail the process that will be followed when an incident commander determines that an interoperability resource is required and a radio cache is determined to be the appropriate resource. This section should define what information is provided during the interoperable communications request, how the request will be handled by dispatch and who will be responsible for determining what interoperability resource should be deployed to the scene. Assuming a radio cache is determined to be the most appropriate resource, this section should specify whether any parties need notification that the particular radio cache has been activated for an incident.

Example: The following is an example of the process that might be followed by a region during an Interoperable Communications Request involving swapping radios.

A. The Incident Commander will determine when a situation exists that requires use of a regional interoperability resource and notify his/her dispatch center.

B. The dispatch center having jurisdiction over the location of the incident follows internal agency procedures to contact a Regional Interoperability Coordinator and relays pertinent information regarding the event.

C. The following information is provided by the requesting agency at the time of an activation request:
   - User's agency
   - On-scene agencies requiring interoperability
   - Reason for request / type of event
   - Expected duration of event
   - User/requestor contact phone number

D. In the event that the agency activates its own radio cache, the Regional Interoperability Coordinator is notified and provided the above information.

E. The Regional Interoperability Coordinator determines what regional interoperability resources are available for use and identifies a specific resource. The Regional Interoperability Coordinator activates the appropriate resource. For example, if a radio cache is activated, the Regional Interoperability Coordinator contacts the Radio Cache Manager to activate the cache.

F. The Regional Interoperability Coordinator coordinates the deployment by providing the contact information for the radio cache to the Incident Commander or their designee.

Radio Cache Activation: This section should detail the process that will be followed during the activation of a radio cache. This section should include how the incident commander will be provided an estimated time of arrival on scene for the radio cache and what process will be used to track the distribution of radios at the incident scene.

Example: The following is an example of the process that might be followed during activation of a radio cache.

A. The Radio Cache Manager will provide an estimated response or activation time, which will be relayed to the dispatch center of the agency having jurisdiction over the event and the Incident Commander.

B. The Radio Cache will be sent to the incident scene along with a knowledgeable technician who will be responsible for supporting the radios, including fully charged spare batteries.

C. Each radio in the radio cache will have a unique identification number for inventory tracking.

D. The technician will be responsible for keeping a list for the incident of each user to whom a radio has been distributed, the agency of the user and the identification number of the radio(s) provided to that individual.

E. Each user and/or agency that has received a radio from the radio cache will be responsible for the return of that radio to the cache at the end of the incident.

Radio Cache Deactivation: This section should detail the process that will be followed during the deactivation of a radio cache. This section should include how the radios will be returned to the radio cache.

Example: The following is an example of the process that might be followed during deactivation of a radio cache.

A. The Incident Commander determines when the regional interoperability asset is no longer required.

B. The Incident Commander or Logistics Section Chief will be responsible for coordinating the return of cache radios to the on scene Radio Cache Technician.

C. At the end of the incident, the Radio Cache Technician will be responsible for inventorying all radios returned to the cache. Before leaving the incident scene, the technician will determine if any radios have not been returned to the radio cache and note the user and/or agency to which the radio was distributed. This information will be provided to the Incident Commander or Logistics Section Chief. If the missing radios can not be recovered at the incident scene, the technician will provide this information to the Radio Cache Manager for resolution.

Problem ID and Resolution: This section should detail the process that will be followed for problem identification and resolution associated with the use of a radio cache.

Example: The following is an example of a process for problem identification and resolution.

A. Agencies using radio caches may report any problems with the specific radio cache to the Regional Interoperability Committee. See Appendix A for Point of Contact information for the Regional Interoperability Committee.

B. The Regional Interoperability Committee will be responsible for ensuring effective resolution to problems that exist with interoperability resources.

2) Shared Channels:

Shared channels refer to common frequencies or channels (such as those of a participating agency) that have been established and are programmed into radios to provide interoperable communications among agencies. In order to use this option adequately, *all user radios must be capable of operating on the same channel.* Shared channels and shared systems are the only types of interoperable communications equipment that are always available because they are included and always operational in each piece of equipment.

The National Law Enforcement Emergency Channel (155.475 MHz) is an example of a shared channel available for use in the region if all agencies are using the VHF High Band.

If shared channels are available for use by the region, the specific channels and their purpose should also be documented in Appendix C.

Rules of Use: The following are some rules of use that may be included in this section. These examples are not exhaustive. The region should include any rules of use in this section that will apply to shared channels, including:

- National Incident Management System compliance.
- Use of plain language (no radio codes).
- Use of Unit Identification.
- Use of encryption / no encryption.

NOTE: Based on best practices / lessons learned from emergency responders, encryption should be used only if the agencies involved have established that it will not prevent successful interoperability.

Procedures: This section should detail the process that will be followed when an incident commander determines that an interoperability resource is required and a Shared Channel is determined to be the appropriate resource. This section should specify if anyone should be notified when a Shared Channel resource will be required for a significant amount of time in order to support a particular incident.

Example: The following is an example of the procedure that might be followed by a region during use of a Shared Channel.

A. If an individual responder needs to talk to an agency with whom they do not otherwise have communications, the responder notifies dispatch that they need to operate on one of the interoperability channels. Dispatch or the responder can determine the appropriate channel.

B. For an extended incident, the dispatcher is responsible for notifying the regional Interoperability Coordinator that an interoperability or mutual aid channel is in use.

C. When a responder is dispatched to an incident, each agency dispatcher is responsible for notifying responders what interoperability channel or channels are being used for the incident.

D. The Incident Commander determines when the interoperability or mutual aid channel(s) is (are) no longer required and notifies his/her dispatch center.

E. The dispatch center having jurisdiction over the location of the incident notifies each responding agency that operations on the channel are ending.

Problem Identification & Resolution: This section should detail the process that will be followed for problem identification and resolution associated with the use of shared channel.

Example: The following is an example of a process for problem identification and resolution.

A. The dispatch center having jurisdiction over the location of the incident reports any problems experienced to the Regional Interoperability Committee. See Appendix A for Point of Contact information for the Regional Interoperability Committee.

B. The Regional Interoperability Committee will be responsible for ensuring effective resolution to problems that exist with interoperability resources.

3) Gateways:

Gateway systems provide connections between two or more radio networks, allowing users on one network to communicate with users on other networks. For example, a group of users on an ultra-high frequency (UHF) channel used by Agency A can be connected to a group of users on a very-high frequency (VHF) channel used by Agency B. An interconnect is created by connecting two or more radio channels or voice paths with a gateway device or console patch. Gateway systems can be configured to support any number of channels. Using gateway systems, usually graphical user interface, a dispatch operator can select the appropriate channels to interconnect. With many gateways, multiple interconnect sessions involving distinct groups can be established at any given time by the gateway operator. The maximum number of simultaneous interconnect sessions in progress depends on the gateway system. Examples of gateways include M/A-Comm's Network First, Raytheon's JPS ACU-1000 and Sytech's RIOS.

Gateway systems are typically used in regions where there is overlapping coverage of participating radio communications systems. For example, two

agencies responding to an incident can have channels from their respective communications networks interconnected, but this is only useful if the coverage area of each network includes the incident location. An agency must be able to access its own communications network. Thus, the service areas for a gateway system is generally restricted to the overlapping service area of all participating agencies in any given interconnect.

Participating Agencies: Using Appendix D, jurisdictions should list which agencies will be included in the use of gateway solutions.

NOTE: Gateway systems require a separate channel for each participating agency. For example, a gateway system may be used to connect Agency A on UHF channel 1 with Agency B on UHF channel 2 and Agency C on UHF channel 3. The interconnect then involves three channels, or one for each agency. If an agency only has a limited number of channels, it should realize that a high percentage of its communications resources are being devoted to the shared operation.

Rules of Use: The following are some rules of use that may be included in this section. These examples are not exhaustive. The region should include any rules of use in this section that will apply to gateways, including:

- National Incident Management System compliance.
- Use of plain language (no radio codes).
- Use of Unit Identification.
- Use of encryption / no encryption.

NOTE: Based on best practices / lessons learned from emergency responders, encryption should be used only if the agencies involved have established that it will not prevent successful interoperability. Gateways do not adequately support encryption and voice quality through the interconnect can suffer significantly. The agencies engaged in arrangements using gateways should ensure that their agreements and technical setup are compliant with FCC rules and regulations.

Interoperable Communications Request: This section should detail the process that will be followed when an incident commander determines that an interoperability resource is required and a gateway is determined to be the appropriate resource. This section should define what information is provided during the interoperable communications request, how the request will be handled by dispatch and who will be responsible for determining what interoperability resource should be deployed to the scene. Assuming a gateway is determined to be the most appropriate resource, this section should also specify whether any parties need notification that the particular gateway has been activated for an incident.

Example: The following is an example of the process that might be followed by a region during an Interoperable Communications Request involving a gateway. Note that this process assumes that specific individuals will be appointed to the role of Regional Interoperability Coordinators. This process also assumes that there is a designated manager for each gateway device.

A. The Incident Commander determines when a situation exists that requires use of a regional interoperability resource and notifies his/her dispatch center.

B. The dispatch center having jurisdiction over the location of the incident follows internal agency procedures to contact the Regional Interoperability Coordinator and relays pertinent information regarding the event.

C. The following information is provided by the requesting agency at the time of an activation request:

- User's agency
- Agencies or frequencies / talk groups to connect
- Reason for request / type of event
- Expected duration of event
- User / requestor contact phone number

D. In the event that the agency activates its own gateway, the Regional Interoperability Coordinator is notified and provided the above information.

E. The Regional Interoperability Coordinator determines what regional interoperability resources are available for use and identifies a specific resource. The Regional Interoperability Coordinator activates the appropriate resource. For example, if a gateway is activated, the Regional Interoperability Coordinator contacts the Gateway Manager to activate that device.

F. The Regional Interoperability Coordinator coordinates the deployment by providing the contact information for the gateway to the Incident Commander or their designee.

Gateway Activation: This section should detail the process that will be followed during the activation of a gateway. If a mobile gateway will be deployed to the scene of the incident, this section should include how the incident commander will be provided an estimated time of arrival for the resource. For all gateways (i.e. fixed or mobile configurations) this section should detail: what authorizations have to be obtained before interconnecting agency channels; how the Incident Commander, or designee (such as the Communications Unit Leader), is notified that the interconnects have been established; and, how users on affected channels are notified prior to the interconnect that routine use of the channel will be suspended so that the channel can be used to support the response to an incident.

Example: The following is an example of the process that might be followed during activation of a Gateway.

A. The Gateway Manager advises an estimated response or activation time, which is relayed to the dispatch center of the agency having jurisdiction over the event and the Incident Commander.

B. The responding Gateway Manager establishes contact with the Incident Commander, or his/her designee, to consult on any issues concerning the radio interconnect.

C. Verbal authorization is necessary from each agency before interconnects are activated. The Regional Interoperability Coordinator is responsible for obtaining those authorizations and ensuring the interconnects will serve the intended need. Any agency may deny authorization to activate an interconnect at any time, for any reason.

D. The Gateway Manager notifies the dispatcher that the interconnect has been prepared.

E. If the Gateway Manager is not on-scene, the dispatcher notifies the Incident Commander that the interconnect has been prepared.

F. The Gateway Manager ensures an announcement has been made on each interconnect to notify existing users on affected channels that these resources will be interconnected to support an incident.

G. The Gateway Manager is responsible for the gateway operation until such time as the deployment is terminated or the event is handed off to another Gateway Manager.

Gateway Deactivation: This section should detail the process for identifying who will decide when the Gateway is no longer required to support the incident and how each agency will be notified prior to the disconnection of channels from each interconnect.

Example: The following is an example of the process that might be followed during deactivation of a Gateway.

A. The Incident Commander determines when the regional interoperability asset is no longer required and notifies his/her dispatch center.

B. The dispatch center having jurisdiction over the location of the incident notifies each connected agency that the interconnect will be deactivated.

C. The Gateway Manager makes an announcement on each interconnect to notify existing users on affected channels that these resources will be disconnected. The resource is then deactivated after allowing time for alternate communication arrangements, if needed.

Problem Identification and Resolution: This section should detail the process that will be followed for problem identification and resolution associated with the use of a Gateway.

Example: The following is an example of a process for problem identification and resolution.

A. The Gateway Manager reports any problems experienced during the deployment to the Regional Interoperability Committee following the incident. Agencies using Gateways may also report any problems experienced. See Appendix B for Point of Contact information for the Regional Interoperability Committee.

B. The Regional Interoperability Committee will be responsible for ensuring effective resolution to problems that exist with interoperability resources. The Gateway Manager immediately reports any problems with activation of the interconnects to the Incident Commander and the Regional Interoperability Coordinator.

4) Shared Systems:

Shared systems refers to the use of a single radio system infrastructure to provide service to most agencies within a region. Shared systems are typically built upon a trunking architecture. The region should only list a shared system as an available interoperability resource if the majority of public safety users within the region share a common system. In the case where less than a majority of public safety uses a shared system, there may be several incompatible systems shared by subsets of users within the region. Possession of a single radio system allows subsets of users to achieve interoperability, however for the purposes of this document, shared systems should only be listed if they have a significant impact on region-wide, public-safety interoperability.

If a shared system is available for use by the region, the system should be documented in Appendix E.

Rules of Use: This section should detail the process that will be followed when an incident commander determines that an interoperability resource is required and a shared system channel/talk group is determined to be the appropriate resource. This section should specify if anyone should be notified when a Shared System resource will be required for a significant amount of time in order to support a particular incident. The region should develop a standard set of rules of use for common channel/talkgroup assignment and document these in this section. Importantly, this is one of two types of interoperability solutions that can have an "automatic deployment" based upon the occurrence of an incident (such as a law enforcement pursuit) because the resource is always available in all participating radios; the other always-available solution is Shared Channels for this same reason. The following are some rules of use that may be included in this section. These examples are not exhaustive. The region should include any rules of use in this section that will apply to gateways, including:

- National Incident Management System compliance
- Use of plain language (no radio codes)
- Use of Unit Identification
- Use of encryption / no encryption

NOTE: Based on best practices / lessons learned from emergency responders, encryption should be used only if the agencies involved have established that it will not prevent successful interoperability. Shared systems may be the only interoperability solution in the region. Because encrypted channels/talk groups are already programmed into user's radios, they are available to support protected communications. However, their successful use may be limited to within a particular discipline or on designated interoperability talk groups such as for Incident Commanders.

Example: The following is an example of the procedure that might be followed by a region during use of a Shared System.

A. If an individual responder needs to talk to an agency with whom they do not otherwise have communications, the responder notifies dispatch that they need to operate on one of the interoperability channel. Dispatch or the responder can determine the appropriate channel/talkgroup.

B. For an extended incident, the dispatcher is responsible for notifying the regional Interoperability Coordinator that an interoperability channel/talkgroup is in use.

C. When a responder is dispatched to an incident, each agency dispatcher is responsible for notifying responders what interoperability channel(s)/talkgroup(s) being used for the incident.

D. The Incident Commander determines when the interoperability channel/talkgroup is (are) no longer required and notifies his/her dispatch center.

E. The dispatch center having jurisdiction over the location of the incident notifies each responding agency that operations on the channel/talkgroup are ending.

Problem Identification & Resolution: This section should detail the process that will be followed for problem identification and resolution associated with the use of a Shared System.

Example: The following is an example of a process for problem identification and resolution.

A. The dispatch center having jurisdiction over the location of the incident reports any problems experienced to the Regional Interoperability Committee. See Appendix B for Point of Contact information for the Regional Interoperability Committee.

B. The Regional Interoperability Committee will be responsible for ensuring effective resolution to problems that exist with interoperability resources.

Section 5 – Plans for Tactical Communications During IED Incident

For the purpose of this Tactical Interoperable Communications Plan, utilize the scenario of an Improvised Explosive Device (IED) detonated in a crowded venue.

1) Participating Disciplines:

Document the functional disciplines to which this Tactical Interoperable Communications Plan applies. For the purposes of satisfying the requirements of the FY05 UASI grant, this Tactical Interoperable Communications Plan is intended to apply to first responders. In particular, it should apply to functional disciplines that would be involved on-scene in the first 12 hours of the response to a terrorist event.

2) Planned Use of Interoperable Equipment:

Document how available interoperability equipment will be used within the NIMS structure to support the response to an incident. Standard ICS 205 forms or the equivalent should be included to show functional assignments of communications resources.

The method of interoperable communications to be used during an incident should be included for each of the following:

- Incident Command and General Staff
- Operations Section, including separate functional groups or geographic divisions
- Planning Section
- Logistics Section
- Finance Section (if established)

Depending on the equipment listed in Section 3 – Interoperability Equipment, any of the following methods might be used to provide communications capabilities to these groups:

- Swap Radios from a radio cache could be distributed to the Logistics Section members to allow them to communicate using compatible radios.
- A Shared Channel or Channels could be assigned to provide required interoperability.
- A Gateway could be used to interconnect channels from the respective agencies or systems.
- Shared System resources (i.e. talk groups) could be established to support required communications among the agencies.

NOTE: While not required to fulfill the Tactical Interoperable Communications Plan requirement of the FY05 HSGP grant, agencies are encouraged to develop additional communications plans to address other terrorism scenarios.

Section 6 – Training

Training and exercises refers to the instructional support designed to develop knowledge, skills, and performance of public safety personnel. Proper training and regular exercises are critical to the implementation and maintenance of a successful interoperability solution. Success will be assured by regular, comprehensive, and realistic exercises that address potential problems in the region and involve the participation of all relevant personnel. Without training and exercises, emergency responders will not be able to effectively use the technology in the event of a major incident.

The two-way radio is today one of a public safety officer's most used pieces of equipment – as important to the firefighter as a breathing apparatus and to the police officer as a handgun. Unfortunately, while training and certification is routinely required for these latter pieces of equipment, it is rarely provided for radio equipment particularly with regard to interoperability. A radio will do no good when needed to respond to an incident if the public safety officer does not know how to use it.

Proper training and regular exercises are critical to the implementation of a successful interoperability solution. Federal guidance now requires agencies to implement the National Incident Management System (NIMS) program for incident management. Issued on March 1, 2004, NIMS provides a consistent nationwide approach for federal, state, territorial, tribal, and local governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

For FY2005, state and territory level efforts to implement NIMS must include the following:

- Incorporating NIMS into existing training programs and exercises.
- Ensuring that federal preparedness funding, including Homeland Security Grant Program (HSGP) funds, support NIMS implementation at the state and local levels (in accordance with eligibility and allowable uses of grants).
- Incorporating NIMS into Emergency Operations Plans (EOPs).
- Promotion of intrastate mutual aid agreements.
- Coordinating and providing technical assistance to local entities regarding NIMS.
- Institutionalizing the use of Incident Command System (ICS).

By FY07, federal preparedness assistance will be conditioned upon full compliance with NIMS.

First responder communications training typically takes place during a responder's initial basic training, and then infrequently throughout the first responder's career. It is the intent of the NIMS guidelines to promote more thorough and frequent training on all aspects of multi-agency incident response, and in particular those involving such critical issues as communications. This Tactical Interoperable Communications Plan should document efforts to provide routine communications training, including training for use of interoperable communications resources.

Finally, no technical solution will work without trained support staff. The state and/or urban area must ensure that sufficient personnel are trained as Communications Unit Leaders, as defined within NIMS, to support equipment deployment. As part of this Tactical Interoperable Communications Plan, agency personnel are required to document the disciplines and numbers of certified Communications Unit Leaders. The Tactical Interoperable Communications Plan should address staffing to ensure that Communications Unit Leaders are available at all times (24/7).

Assistance Available from ODP

ODP's Interoperable Communications Technical Assistance Program (ICTAP) was established to address the public safety community's inability to communicate between agencies during an emergency. This lack of communications capability between multiple jurisdictions, as well as across the different emergency responder disciplines, results largely from agencies having its own unique legacy technologies, targets, requirements, operating environments, laws, and processes.

ICTAP is available on a first-come, first-serve basis to provide technical assistance at no cost to States and Urban Areas. The ICTAP team developed this Guidance document and has a staff of policy, technical and operational personnel to assist in both the development and implementation of the required Tactical Interoperable Communications Plan.

ICTAP can support a region's efforts to develop its Tactical Interoperable Communications Plan through the following services:

- Assist in developing the technical content and operational procedures for Tactical Interoperable Communications Plans.
- Facilitate meetings.
- Review Tactical Interoperable Communications Plans prior to submission.

Once the Tactical Interoperable Communications Plan is developed, further assistance from ICTAP can be requested through ODP to support implementation and validation of the plan. The following services may be available, based on each region's needs:

- Providing a baseline assessment of current interoperability capabilities and communications infrastructure through the use of the Communications Asset Surveying and Communication Assets Mapping Tools.
- Performing interoperability gap analysis.
- Providing recommendations and suggested solutions for gap reduction.
- Validating operational procedures and Tactical Interoperable Communications Plans through table top exercises.
- Conducting technical feasibility studies to support the development of regional interoperability systems.
- Assisting in the development of a training plan for interoperable communications.
- Providing technical assistance in the development of regional short and long-term interoperability plans.

In many States and Urban Areas, ICTAP participates as a member of UASI Working Groups. The ICTAP team provides guidance, as well as technical studies to support ongoing efforts to improve interoperability for the region(s).

ICTAP assistance may be requested through your ODP Preparedness Officer, or by contacting the ODP Centralized Scheduling and Information Desk (CSID) at 1-800-368-6498, or via e-mail at askcsid@dhs.gov.

Tactical Interoperable Communications Plan Template

Section 1. Urban Area Information

1.1 Overview

Provide a brief overview information on the Urban Area and its efforts to date addressing interoperable communications.

1.2 Included Agencies

List the agencies represented in the Tactical Interoperable Communications Plan. For UASI grantees, this must include all agencies included in the Urban Area Working Group (UAWG).

1.3 Tactical Interoperable Communications Plan Point of Contact

Name a primary point of contact (POC) that can be reached for questions regarding the plan.

- Name _____
- Title _____
- Address _____
- Phone _____
- E-Mail _____

Section 2. Governance

2.1 Overview

Provide a brief overview of the governance structure that oversees interoperable communications policy.

2.1 Membership

Complete Appendix A which provides a template by which to provide POC information on members of the governing body.

Section 3. Interoperability Equipment

SAFECOM defines communications interoperability as the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when needed, and as authorized. All interoperable equipment in the grantee's region should be listed according to the following categories:

3.1 Swap Radio

Provide a list of all swap radios and the agencies that are making these resources available.

3.2 Shared Channel

Provide a list of all shared channels and the agencies to which these channels are available.

3.3 Gateway

Provide a list of all gateway systems and the agencies that are making these resources available.

3.4 Shared System

Provide a list of all shared systems and the agencies to which these systems are available.

Section 4. Policies & Procedures for Interoperable Equipment

4.1 Swap Radios

This section should be completed only if the region has included the use of Swap radios in the Plan.

- **Technology Overview**
  Provide background information on swap radios and their role in the regional plan.

- **Rules of Use**
  Develop a standard set of rules of use for radio caches and document these in this section.

- **Interoperable Communications Request**
  Detail the process that will be followed when an incident commander determines that an interoperability resource is required and a radio cache is determined to be the appropriate resource.

- **Radio Cache Activation**
  Detail the process that will be followed during the activation of a radio cache.

- **Radio Cache Deactivation**
  Detail the process that will be followed during the deactivation of a radio cache.

- **Problem ID and Resolution**
  Detail the process that will be followed for problem identification and resolution associated with the use of a radio cache.

4.2 Shared Channels

This section should be completed only if the region has included the use of shared channels in the Plan.

- **Technology Overview**
  Provide background information on shared channels and their role in the regional plan.

- **Rules of Use**
  Detail a standard set of rules of use for radio caches.

- **Procedures**
  Detail the process that will be followed when an incident commander determines that an interoperability resource is required and a shared channel is determined to be the appropriate resource.

- **Problem ID and Resolution**
  Detail the process that will be followed for problem identification and resolution associated with the use of a radio cache.

4.3 Gateways

This section should be completed only if the region has included the use of Gateways in the Plan.

- **Technology Overview**
  Provide background information on gateways and their role in the regional plan.

- **Participating Agencies**
  Use Appendix D to list the agencies supported by each gateway device.

- **Rules of Use**
  Detail a standard set of rules of use for gateways and document these in this section.

- **Interoperable Communications Request**
  Detail the process that will be followed when an incident commander determines that an interoperability resource is required and a gateway is determined to be the appropriate resource.

- **Gateway Activation**
  Detail the process that will be followed during the activation of a gateway.

- **Gateway Deactivation**
  Detail the process that will be followed during the deactivation of a gateway.

- **Problem ID and Resolution**
  Detail the process that will be followed for problem identification and resolution associated with the use of a gateway.

4.4 Shared Systems

This section should be completed only if the region has included the use of Shared Systems in the Plan.

- **Technology Overview**
  Provide background information on shared systems and their role in the regional plan.

- **Rules of Use**
  Detail a standard set of rules of use for gateways and document these in this section.

- **Procedures**
  Detail the process that will be followed when an incident commander determines that an interoperability resource is required and shared systems are determined to be the appropriate resource.

- **Problem ID and Resolution**
  Detail the process that will be followed for problem identification and resolution associated with the use of shared systems.

Section 5. Plans for Tactical Communications During an Incident

5.1 Participating Functional Disciplines

List the functional disciplines to which the Tactical Interoperable Communications Plan applies.

5.2 Plan for Tactical Use of Interoperability Resources

Document how available interoperability resources will be used within the ICS structure to support the response to an incident. Prepare sample incident communications plans (ICS 205 or equivalent) showing functional assignments of resources, including:

- **Incident Command**
  Detail what method or specific interoperability resources will be used for communication among the Incident Command Staff and with other Sections General Staff.

- **Operations Section**
  Detail what method or specific interoperability resources will be used for communication within the Operations Staff and with other Sections Operations Staff.

- **Planning Section**
  Detail what method or specific interoperability resources will be used for communication within the Planning Section and with other Sections.

- **Logistics Section**
  Detail what method or specific interoperability resources will be used for communication within the Logistics Section and with other Sections.

- **Finance Section**
  While often not activated until later in a major incident (typically during the recovery phase), maintenance of detailed equipment and personnel activities and expenditures is critical for disaster reimbursement. If there is a communications requirement for this Section, detail what method or specific interoperability resources will be used for communication within the Finance Section and with other Sections.

Section 6. NIMS Training

Detail your progress and future plans to ensure that adequate staff are trained as Communications Unit Leaders as defined by the NIMS model.

Glossary

Agency: An agency, for the purposes of this document, is a group of radio users organized by political subdivision or response organization.

Gateway Agency: A public safety agency that has acquired a fixed or mobile gateway device and agrees to abide by the policies established by the Public Safety Communications Board.

Gateway Manager: The Gateway Manager shall be the responsible party within a public safety or public service entity trained for use, operation and deployment of a Gateway (fixed or mobile). The Gateway Manager may deploy one or more subordinate technicians who will act under their supervision and control.

Gateway System: Any communication network set up that involves the utilization of one or more Gateway devices (e.g., ACU-1000).

Incident Command System (ICS): The coordinated effort of managing emergency responders that requires functionality outside the scope of the normal job routine. Incident Command is the first requirement to utilizing any interoperability function within the regional communications system. The Incident Command Structure commences on the field responder level and involves field supervision authority called the Incident Commander. See also *National Incident Management System*.

Incident Commander: The Incident Commander provides the field supervision authority during an incident as outlined in the *National Incident Management System*.

Interconnect: An interconnect is created by connecting two or more radio channels or voice paths with a gateway device, VoIP interconnection or console link.

Interoperability Resources: The devices and systems in use in the region to enable communications interoperability.

National Incident Management System (NIMS): Guidelines developed by the first responder community and endorsed by national first responder associations and the Department of Homeland Security to establish a consistent nationwide approach to a core set of concepts, principles and standard terminology for incident management. The core concepts include: the Incident Command System (ICS); multi-agency coordination systems; training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

Public Safety Answering Point (PSAP): A facility equipped and staffed to field emergency calls, such as 911.

Public Safety Communications Board: Group established to set public safety policies and to oversee their implementation/execution.

Regional Incident Management: Routine coordination of responses across a region to natural and technological disasters and attacks.

Regional Interoperability Committee: The committee established in the region to oversee regional communication issues.

Regional Interoperability Coordinator: Executes the day-to-day oversight and coordination of regional interoperable communications resources.

Unit: A unit is the individual radio subscriber belonging to an agency and maintaining a specific radio identity.

Appendix A Governance Contacts

In this appendix, the region should include points of contact for governance entities as well as any individuals appointed for regional coordination of interoperability resources.

The examples used in this document would be supported by the following list of contacts:

- Public Safety Communications Board
  Joe Smith
  Director, Public Safety Communications Board
  (909)555-1111
  joe.smith@email.com

- Regional Interoperability Committee
  Henry Block
  Director, Regional Interoperability Committee
  (909)555-2222
  henry.block@email.com

- Regional Interoperability Coordinator(s)
  Susan Lee
  Regional Interoperability Coordinator
  (909)555-3333
  susan.lee@email.com

Appendix B Swap Radios Template

For each radio cache listed in Section 3, complete a form similar to the one below.

B1 Equipment Location

The location of the radio cache will be entered in this section. For example, "This radio cache is maintained at the City A Police Department Headquarters at 75th & State Street."

B2 Responsible Agency

The agency and point of contact responsible for this Radio Cache will be entered in this section. For example, "This radio cache is operated by the City A Police Department. The contact for this system follows."

City A Police Department
Communications Manager
(909) 555-5555

B3 Service Area

Information regarding the area in which this radio cache is available to be deployed would be entered in this section. For example, "This system is available for use throughout Alpha, Bravo and Charlie counties."

B4 Cache Description

The number of radios and spares will be provided in this section. Additionally, a description should be provided of the radio type and programmed channels. For example, "This radio cache consists of 100 VHF radios with 100 fully charged battery spares. The radios support 16 channels. The following channels are currently programmed:

Channel 1 - City A Tactical 1 (156.265)

Channel 2 - City A Tactical 2 (156.280)

Channel 3 - City A Tactical 3 (156.295)

Channel 4 - National Fire Mutual Aid (154.265)

Channel 5 - National Fire Mutual Aid (154.280)

Channel 6 - National Fire Mutual Aid (154.295)

Channel 7 - The National Law Enforcement Emergency Channel (155.475)

Channels 8 through 16 – Unassigned

Appendix C Shared Channels Template

For each shared channel listed in Section 3, complete a form similar to the one below.

C1 Frequencies

List the frequencies for the shared channel or group of channels. For example, "The National Fire Mutual Aid frequencies are 154.265, 154.280 and 154.290MHz.

C2 Purpose

Specify the intended use for the channels. For example, "The FCC has set aside these frequencies as National Fire Mutual Aid frequencies. These frequencies are used for Fire Department operations, search and rescue, evacuation, and to facilitate alerting and warning the general public."

C3 Notes

List any other notes, for example restrictions or limitations on use of the channels.

Appendix D Gateways Template

For each gateway listed in Section 3, complete a form similar to the one below.

D1 Equipment Location

The location of the radio cache will be entered in this section. For example, "This radio cache is maintained at the City A Police Department Headquarters at 75th & State Street."

D2 Responsible Agency

The agency and point of contact responsible for this Radio Cache will be entered in this section. For example, "This radio cache is operated by the City A Police Department. The contact for this system follows."
City A Police Department
Communications Manager
(909) 555-5555

D3 Service Area

Information regarding the area in which this Radio Cache is available to be deployed would be entered in this section. For example, "This system is available for use throughout Alpha, Bravo and Charlie counties."

D4 System Capacity

Information regarding the number of users that can be interconnected at a given time would be included in this section. For example, "This gateway system can support up to 24 active channels involved in up to 7 interconnects."

D5 Participating Agencies

Information on the agencies and channels supported on the particular gateway system will be included in this section.

Agency	Channel Designation
Agency A	Agency A Tactical 1
Agency B	Agency B Tactical 1
Agency C	Agency B Tactical 1
etc.	

Appendix E Shared Systems Template

For each shared system listed in Section 3, complete a form similar to the one below.

E1 System Designation

Identify how the system is designated or referred to. For example, "This system is referred to as the County A Trunked Radio System."

E2 System Type

List the make and model of the shared system used within the region.

E3 Responsible Agency

List the agency or entity responsible for the shared system, along with point of contact information. For example, "This radio cache is operated by the City A Police Department. The contact for this system follows."

City A Police Department
Communications Manager
(909) 555-5555

E4 Service Area

Describe in general terms the area served by the shared system. The service area may be described with a statement such as, "The shared system serves three of the four counties surrounding the metropolitan core area."

E5 Participating Agencies

List the agencies using the shared system.